AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Oregon

Eugene Division

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	)	Case No. 6:16-MC- 240
A light colored trailer; a white Toyota Camry, bearing Idaho license plate 1A2852B; and a Ford Pickup truck, bearing Idaho license plate 1A2549N as further described in Attachment A	)	

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Oregon

(identify the person or describe the property ta be searched and give its location):

A light colored trailer; a white Toyota Camry, bearing Idaho license plate 1A2852B; and a Ford Pickup truck, bearing Idaho license plate 1A2549N as further described in Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

YOU ARE COMMANDED to execute this warrant on or before 5/18/16 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Thomas M. Coffin, United States Magistrate Judge .

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 5/5/16 2pm

_____

Judge's signature

City and state: Eugene, Oregon

Thomas M. Coffin, U.S. Magistrate Judge

Printed name and title

Return

Case No.: 6:16-MC-	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

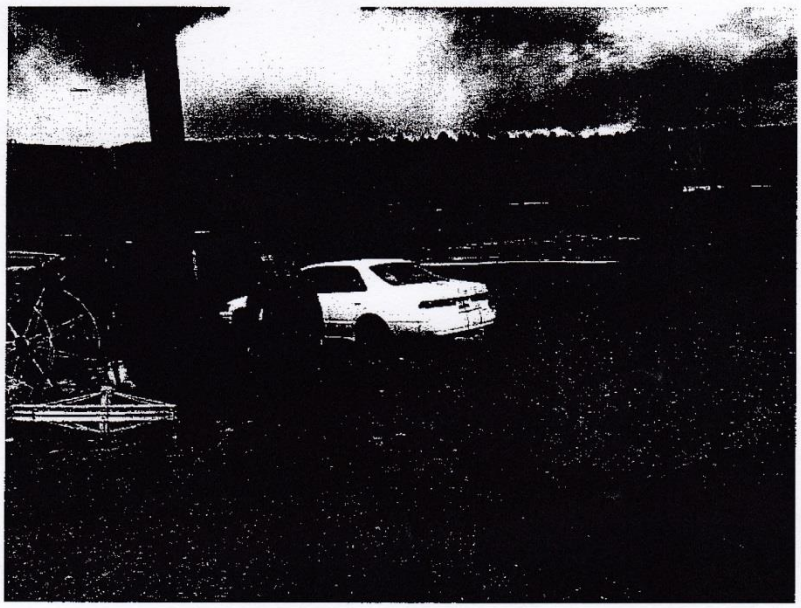
Property to Be Searched

The property to be searched is:

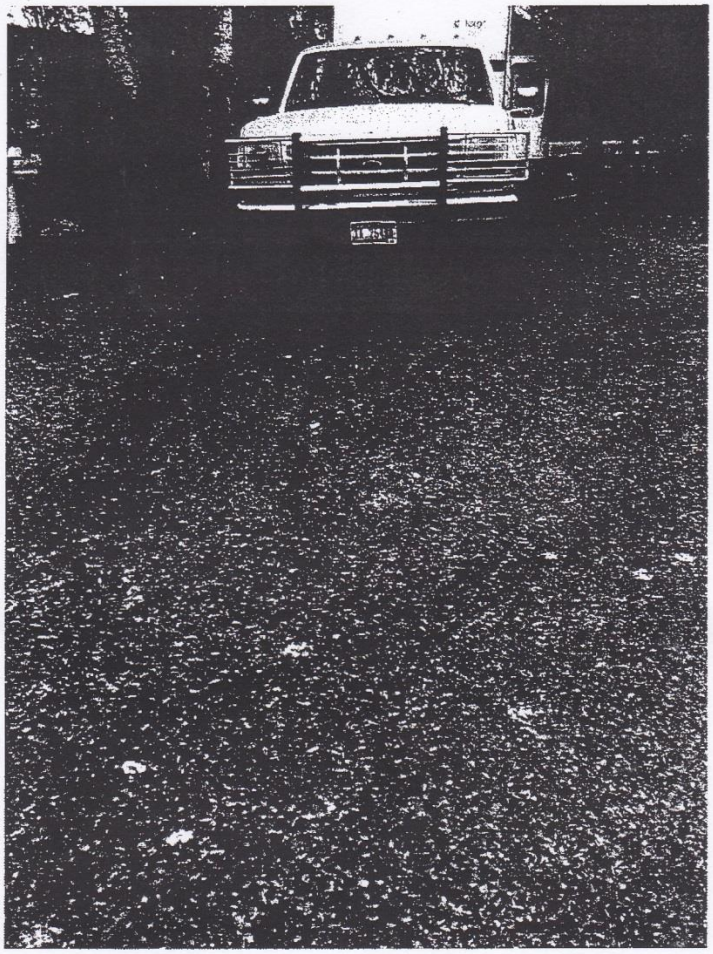
1. A Light colored trailer with the word "Terry" on the front left and rear right corners. The trailer has expired temporary plates that say 4/30/2016 and is further identified in this picture. This trailer was last seen on May 5, 2016 parked in lot 6 411 NW Bridge St, John Day, Oregon 97845.

This trailer was verified at this location in the morning of 5/5/2016. As the trailer is mobile and EMRY owns a truck capable of towing it, this warrant will be valid for the trailer at any location within the District of Oregon.

2. A white Toyota Camry, Idaho License Plate 1A2852B, further identified in this picture:



3. A light-colored Ford pickup, Idaho license plate 1A2549N, further identified in this picture:



ATTACHMENT B

Items to Be Seized

The items to be searched for, seized, and examined, are those items in the trailer and vehicles described in Attachment A, that contain evidence, contraband, fruits, and instrumentalities of violations of 26 U.S.C. §§ 5861(d), 5861(e), and 5861 (f), as follows:

A. <u>Physical Evidence</u>

1. Firearms, to include: handguns, rifles, shotguns, the frames and receivers thereof, ammunition magazines, parts for firearms and firearm boxes. This also includes firearms required to be registered in the National Firearms Registration and Transfer Record, including machine guns, short-barrel rifles/shotguns, silencers and destructive devices;

2. All firearm records, documents, diagrams, manuals, photographs, undeveloped film and videos;

3. Receipts, memoranda, notes, calendar books, log books, appointment books, customer information and vendor information pertaining to the acquisition, receipt, purchase or disposition of firearms. Further items and documentation regarding profit and livelihood from the sale of firearms including records of credit card and automatic teller machine activity including credit and/or debit cards, automatic teller machine records, bank statements, duplicate checks, bank deposit records, bank debits, cashier's checks and money order records, wire transfer records, copies of tax returns, United States currency and other monetary instruments;

4. Any records that establish the person(s) who have control, possession, custody or dominion over the property from which evidence is seized, such as: personal mail, checkbooks, personal identification, notes, other correspondence, utility bills, rent receipts, payment receipts, financial documents, leases, mortgages, bills, records or keys showing possession of safes

and other types of storage areas, including passwords and/or access codes for access during the searches.

As used above, the terms records, documents, programs, applications or materials includes records, documents, programs, applications or materials created, modified, or stored in any form including digital or electronic form.

B. Digital Evidence

1. Any computer equipment or digital devices that are capable of being used to commit or further the crimes outlined above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such crimes, as set forth in this attachment;

2. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes outlined above, or to create, access, process, or store evidence, contraband, fruits, or instrumentalities of such crimes, as set forth in this attachment;

3. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and cell phones capable of being used to commit or further the crimes outlined above, or to create, access, or store evidence, contraband, fruits, or instrumentalities of such crimes, as set forth in this attachment;

4. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

5. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

6. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

7. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data; and

8. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during any time period in which the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

9. As used in this attachment, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

10. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital devices that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter

"Computer"):

a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

c. Evidence of the lack of such malicious software.

d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user.

e. Evidence indicating the Computer user's state of mind as it relates to the crime under investigation.

f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.

h. Evidence of the times the Computer was used.

i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer.

j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.

k. Records of or information about Internet Protocol addresses used by the Computer.

l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

m. Contextual information necessary to understand the evidence described in this attachment.

n. Routers, modems, and network equipment used to connect computers to the Internet.

Search Procedure

11. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

12. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of

execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

13. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

14. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

15. The government may retain the computer and storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

16. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government

avoided its obligations by destroying data or returning it to a third party.